28 January 1997: To ease review the main IW-D report has been divided into this introductory material and the Executive Summary, and each of the seven sections and appendices listed in the Table of Contents with hyperlinks to each.

8 January 1997

REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON INFORMATION WARFARE - DEFENSE (IW-D)

November 1996

**OFFICE OF THE UNDER SECRETARY OF DEFENSE
FOR ACQUISITION & TECHNOLOGY
WASHINGTON, D.C. 20301-3140**

This report is a product of the Defense Science Board (DSB). The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

This report is UNCLASSIFIED.

DEFENSE SCIENCE BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

25 November 1996

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (ACQUISITION & TECHNOLOGY)

SUBJECT: Report of the DSB Task Force on Information Warfare (Defense)

I am pleased to forward the final report of the DSB Task Force on Information Warfare (Defense), which was chaired by Mr. Duane P. Andrews. You asked the Task Force to focus on protection of information interests of national importance through establishment and maintenance of a credible information warfare (IW) defensive capability in several areas, including deterrence and to make recommendations regarding the creation and maintenance of specific aspects of a national information warfare defense capability.

The Task Force recommends a series of over 50 actions designed to better prepare the Department for this new form of warfare beginning with identification of an accountable focal point within the Department for all IW activities and ending with the allocation or reallocation of approximately $3 billion over the next 5 years to implement these recommended actions.

[Signature]

Craig I. Fields
Chairman

DEFENSE SCIENCE BOARD

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

21 November 1996

Dr. Craig Fields
Chairman
Defense Science Board
3140 Defense Pentagon
Washington, DC 20301-3140

Dear Dr. Fields

Attached is the report of the DSB Task Force on Information Warfare (Defense).

We conclude that there is a need for extraordinary action to deal with the present and emerging challenges of defending against possible information warfare attacks on facilities, information, information systems, and networks of the United States which would seriously affect the ability of the Department of Defense to carry out its assigned missions and functions. We have observed an increasing dependency on the Defense Information Infrastructure and increasing doctrinal assumptions regarding the continued availability of that infrastructure. This dependency and these assumptions are ingredients in a recipe for a national security disaster.

I should also point out that this is the third consecutive year a DSB Summer Study or Task Force has made similar recommendations to better prepare the Department for the challenges of information warfare.

Accordingly, we recommend a series of over 50 actions designed to better prepare the Department for this new form of warfare beginning with identification of an accountable focal point within the Department for all IW activities and ending with the allocation or reallocation of approximately $3 billion over the next 5 years to implement these recommended actions.

We will be, of course, happy to provide any further assistance you may desire.

Sincerely,

[Signature]

Duane P. Andrews

Attachment

PREFACE

The Defense Science Board Task Force on Information Warfare (Defense) was established at the direction of the Under Secretary of Defense for Acquisition and Technology. By USD(A&T) Memorandum for the Chairman, Defense Science Board, dated October 4, 1995, the Task Force was directed to "focus on protection of information interests of national importance through the establishment and maintenance of a credible information warfare defensive capability in several areas, including deterrence." Specifically, the Task Force was asked to:

- Identify the information users of national interest who can be attacked through the shared elements of the national information infrastructure.
- Determine the scope of national information interests to be defended by information warfare defense and deterrence capabilities.
- Characterize the procedures, processes, and mechanisms required to defend against various classes of threats to the national information infrastructure and the information users of national interest.
- Identify the indications and warning, tactical warning, and attack assessment procedures, processes, and mechanisms needed to anticipate, detect, and characterize attacks on the national information infrastructure and/or attacks on the information users of national interest.
- Identify the reasonable roles of government and the private sector, alone and in concert, in creating, managing, and operating a national information warfare-defense capability.
- Provide specific guidelines for implementation of the Task Force's recommendations.

For the purpose of this report, the terms national and national-level are assumed to include Federal, state and local governments, academia, associations, public interest organizations, and the private sector.

This report presents the conclusions and recommendations of the Task Force based on study efforts of the Task Force and Panels created by the Task Force to address specific areas of interest. The report is organized as follows:

- Executive Summary.
- Section 1, Introduction, provides background information.

- Section 2, Environment, describes factors pertinent to the study effort.
- Section 3, Observations, provides the major findings of the Task Force.
- Section 4, What Should We Defend?, identifies the information users of national interest and scope of interests to be defended.
- Section 5, How Should We Defend?, suggests processes and procedures necessary to defend the users against the threats. It includes a discussion of required indications and warning, tactical warning, attack assessment, and continuity of operations organizations and procedures.
- Section 6, Recommendations, presents recommendations, and provides specific guidelines for implementing the recommendations. It includes a discussion of the reasonable roles of government and the private sector and concludes with resources, in addition to current INFOSEC budgets, required to implement the recommendations.
- Section 7, Summary, briefly summarizes the report and suggests some immediate actions.

Appendices are provided as background and resource information. They do not represent a consensus view of the Task Force and recommendations contained in the Appendices are not Task Force recommendations to the Department. Some of the appendices were used in part as input to the main body of this report. Other appendices are provided because they contain useful information for further discussion of matters addressed in the main body of the report.

At about the same time that the Task Force was created, the President signed a major policy directive regarding the protection of critical infrastructures such as telecommunications, electric power, and transportation. This directive resulted in the creation of a Critical Infrastructures Working Group (CIWG) to address the manner in which the directive should be implemented. The CIWG recommendations were implemented with some modification in Executive Order 13010, Critical Infrastructure Protection which was signed by the President on July 15, 1996. E.O. 13010 establishes a President's Commission to, in part,

- Assess the scope and nature of the vulnerabilities of, and threats to, critical infrastructures,
- Determine what legal and policy issues are raised by efforts to protect critical infrastructures, and
- Recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation.

Given these parallel and closely related activities, the Task Force elected to address information warfare (defense) issues and provide conclusions from both the national and Department of Defense perspectives. However, the Task Force recommendations are specifically oriented on the Department of Defense. Department of Defense dependencies on national level activities for information warfare (defense) are provided to the Secretary of Defense for possible transmittal to the President' s Commission for use in their deliberations.

TABLE OF CONTENTS

Section

LIST OF EXHIBITS

Exhibit

EXECUTIVE SUMMARY

The Environment

The national security posture of the United States is becoming increasingly dependent on U.S. and international infrastructures. These infrastructures are highly interdependent, particularly because of the inter-netted nature of the information components and because of their reliance on the national information infrastructure. The information infrastructure depends, in turn, upon other infrastructures such as electrical power.

Protecting the infrastructures against physical and electronic attacks and ensuring the availability of the infrastructures will be complicated. These infrastructures are provided mostly (and in some cases exclusively) by the commercial sector; regulated in part by federal, state, and local governments; and significantly influenced by market forces. Commercial services from the national information infrastructure provide the vast majority of the telecommunications portion of the Defense Information Infrastructure (DII). These services are regulated by Federal and state agencies. Local government agencies regulate the cable television portion of the information infrastructure. Power generation and distribution are provided by very diverse activities -- the Federal government, public utilities, cooperatives, and private companies. Interstate telecommunications are regulated by the Federal Communications Commission, intrastate telecommunications by the state public utilities commissions. Interstate power distribution is regulated by the Federal Energy Regulatory Commission, intrastate power generation and distribution by the state public utilities commissions.

Observations

Information infrastructures are vulnerable to attack. While this in itself poses a national security threat, the linkage between information systems and traditional critical infrastructures has increased the scope and potential of the information warfare threat. For economic reasons, increasing deregulation and competition create an increased reliance on information systems to operate, maintain, and monitor critical infrastructures. This in turn creates a tunnel of vulnerability previously unrealized in the history of conflict.

Information warfare offers a veil of anonymity to potential attackers. Attackers can hide in the mesh of inter-netted systems and often use previously conquered systems to launch their attacks. The lack of geographical, spatial, and political boundaries offers further anonymity and legal and regulatory arbitrage; this lack also invalidates previously established "nation-state" sanctuaries. Information warfare is also relatively cheap to wage, offering a high return on investment for resource-poor adversaries. The technology required to mount attacks is relatively simple and ubiquitous. During information warfare, demand for information will dramatically increase while the capacity of the information infrastructure will most certainly decrease. The law, particularly international law, is currently ambiguous regarding criminality in and acts of war on information infrastructures. This ambiguity, coupled with a lack of clearly designated responsibilities for electronic defense hinders the development of remedies and limits response options.

Exhibit ES-1 shows additional observations.

- Information warfare has been particularly troublesome for the intelligence community
- We lack a common vocabulary
- Resources are focused on classified content and systems
- It is easy to make the IW-D problem too hard
- Acquisition policy and practices pose dilemmas
- However, a lot can be done
- And DoD must start now!

Exhibit ES-1. Observations

What Should We Defend?

The current Administration's national security strategy for the United States suggests that the nation's "economic and security interests are increasingly inseparable" and that "we simply cannot be successful in advancing our interests-political, military and economic-without active engagement in world affairs." In the broad sense, then, the scope of national information interests to be defended by information warfare defense and deterrence capabilities are those political, military, and economic interests. These include the continuity of a democratic form of government and a free market economy, the ability to conduct effective diplomacy, a favorable balance of trade, and a military force that is ready to fight and that can be deployed where needed. These interests are supported by the delivery of goods and services that result from the conduct of functional activities such as manufacturing, governing, banking and finance, and the like. Some of these activities are critical to the nation's political, military, and economic interests. These critical functional activities, in turn, depend on information technology and critical infrastructures such as banking and finance, electric power, telecommunications, and transportation.

In general, U.S. infrastructures are extremely reliable and available because they have been designed to respond to disruptions, particularly those caused by natural phenomena. Redundancy and diverse routing are two examples of design techniques used to improve reliability and availability. However, deregulation and increased competition cause companies operating these infrastructures to rely more and more on information technology to centralize control of their operations, to support critical functions, and to deliver goods and services. Centralization and reliance on broadly networked information systems increase the vulnerabilities of the infrastructures and the likelihood of disruptions or malevolent attacks.

The information users of national interest who can be attacked through the shared elements of the national information infrastructure are those responsible for performing the critical functions necessary for the delivery of the goods and services upon which our political, military, and economic interests depend.

The Department of Defense (DoD) must preserve its ability to fulfill its basic missions. To do that, DoD must be concerned about the ensured operation of the critical functions and the availability of information necessary to fulfill those missions. The intertwined nature of the functions of national interest and supporting infrastructures add to the complexity: there are critical functions which have national security implications and which must be defended; and there are critical portions of the infrastructures which are necessary for the operation of DoD and national functions.

How Should We Defend?

- The concept for defending the information infrastructure and the information components of other critical infrastructures includes the following principles:
- Critical functions must be capable of being performed in the presence of information warfare attacks.
- Some minimum essential infrastructure capability must exist to support these critical functions.
- Point and layered defenses are preferable to area defenses.
- The infrastructure must be designed to function in the presence of failed components, systems, and networks. The risk associated with failed components, systems, and networks must be managed since it cannot be avoided.
- The infrastructure control functions should not be dependent on normal operation of the infrastructure.

- The infrastructure must be capable of being repaired.

The concept for defending is as follows. In the information age as in the nuclear age, *deter* is the first line of defense. This deterrence must include an expression of national will as expressed in law and conduct, a declaratory policy relative to consequences of an information warfare attack against the United States, and an indication of the resiliency of the information infrastructure to survive an attack. Technology to conduct information warfare is simple and ubiquitous; some form of infrastructure robustness and protection is essential. It is technically and economically impossible to *design and protect* the infrastructure to withstand any and all disruptions, intrusions, or attacks (or avoid all risk). The risk can be managed, however, by protecting selected portions of the infrastructure that support critical functions and activities necessary for maintaining political, military, and economic interests. An equally important function is to verify through independent assessments that the design principles are being followed, that protective measures are being implemented where appropriate, and that the information warfare (defense) readiness posture is as reported.

Tactical warning, damage control, attack assessment, and restoration ensures the continuance of these critical functions and activities in the presence of disruptions or attacks. The essence of tactical warning is monitoring, detection of incidents, and reporting of the incidents. Monitoring and detection of infrastructure disruptions, intrusions, and attacks are also an integral part of the defense against information warfare. Providing an effective monitoring and detection capability will require some policy initiatives, some legal clarification, and an ambitious research and development program. The telecommunications infrastructure will be subject to some form of attack and we should have some capability to limit the damage that results and to restore the infrastructure. Little research has been devoted to the basic procedures necessary to contain "battle" damage, let alone the tools which might provide some automated form of *damage control*. Some form of *attack assessment* is essential to determine the impact of an attack on critical functions and the appropriate response to an attack. Restoration of the infrastructure implies some capability to repair the damage and the availability of resources such as personnel, standby services contracts, and the like. The basic functions of monitoring, detection, damage control, and restoration must begin at the lowest possible operating level. Reports of the activity must be passed to regional, DoD, and national-level organizations to establish patterns of activity and to request assistance as needed in damage control and restoration. Finally, some form of *response* to the intrusions or attacks may be necessary to deter future intrusions or attacks. The response could entail civil or criminal prosecution, use of military force, perception management, diplomatic initiatives, or economic mandates. Because response might also involve offensive information warfare, this report does not address it in detail.

Recommendations

The Task Force makes 13 key recommendations as shown in Exhibit ES-2. The Task Force 'considers these recommendations as imperatives.

Bottom Line - DoD has an urgent need to:

1. Designate an accountable IW focal point

2. Organize for IW-D

3. Increase awareness

4. Assess infrastructure dependencies and vulnerabilities

5. Define threat conditions and responses

6. Assess IW-D readiness

7. "Raise the bar" (with high-payoff, low-cost items)

8. Establish a minimum essential information infrastructure

9. Focus the R&D

10. Staff for success

11. Resolve the legal issues

12. Participate fully in critical infrastructure protection

13. Provide the resources

DSB has been urging action on this problem for 3 years!

Exhibit ES-2. Recommendations

In addition, the Task Force made over 50 additional recommendations, which are categorized under these key recommendations. (Note that the first recommendation addresses all of information warfare, not just defensive information warfare.) The Task Force attempted to prioritize these "key recommendations," but in the end decided that portions of all of these key recommendations should be implemented immediately.

The following discussions provide all of the recommendations made by the Task Force. The parenthetical entry following each of the key recommendations identifies the section of the report in which the recommendations are discussed in detail.

1. Designate an accountable IW focal point (6.1). This is the most important recommendation the Task Force offers. The Task Force believes that the Secretary of Defense needs a single focal point charged to provide staff supervision of the complex activities and interrelationships that are involved in this new warfare area. This includes oversight of both offensive and defensive information warfare planning, technology development and resources. The SECDEF should:

> **1a. Designate ASD(C3I) as the accountable focal point for all IW issues.**
>
> > **1a(1). Develop a plan and associated budget beginning in FY 97 to obtain the needed IW-D capability.**

1a(2). Authorize ASD(C3I) to issue IW instructions.

1a(3). Consider establishing a USD(Information).

1b. Establish a DASD(IW) and supporting staff to bring together as many IW functions as possible.

2. Organize for IW-D (6.2). This key recommendation identifies the need for specific IW-D related capabilities and organizations to provide or support the capabilities. While not specifically addressed by the Task Force, virtual organizations that draw on existing assets and capabilities can be established.

2a. Establish a center to provide strategic indications and warning, current intelligence, and threat assessments. The SECDEF should request the DCI to:

2a(1). Establish an I&W/TA center at NSA with CIA and DIA support.

2a(2). Task and resource the Intelligence Community to develop the processes for Current Intelligence, Indications and Warning, and Threat Assessments for IW-D.

2a(3). Encourage the Intelligence Community to develop information-age trade craft, staff with the right skills, and train for the information age.

2a(4). Conduct comprehensive case studies of U.S. offensive programs and a former foreign program to identify potential indicator collection, funding, training, etc,

2a(5). Establish an organization to examine and analyze probable causes of all security breaches.

2a(6). Develop and implement an integrated National Intelligence Exploitation Architecture to support the organization and processes.

In addition, the SECDEF should:

2a(7). Direct the development of IW Essential Elements of Information.

2b. Establish a center for IW-D operations to provide tactical warning, attack assessment, emergency response, and infrastructure restoration capabilities. The SECDEF should:

2b(1). Establish a DoD IW-D operations center at DISA with NCS, NSA, and DIA support.

2b(2). Develop and implement distributed tactical warning, attack assessment, emergency response, and infrastructure restoration procedures.

2b(3). Interface the operations center with Service and Agency capabilities and I&W/TA support.

2b(4). Establish necessary liaison (e.g., with military and government operations centers, service providers, intelligence agencies, and computer

emergency response centers).

2c. The SECDEF should establish an IW-D planning and coordination center reporting to the ASD(C3I) with interfaces to the intelligence community, the Joint Staff, the law enforcement community, and the operations center. This center will: develop an IW planning framework; assess IW policy, plans, intelligence support, allocation of resources, and IW incidents; develop procedures and metrics for assessing infrastructure and information dependencies; and facilitate sharing of sensitive information such as threats, vulnerabilities, fixes, tools, and techniques within DoD and among government agencies, the private sector, and professional associations.

2d. Establish a joint office for system, network and infrastructure design. This office will: develop and promulgate IW-D policies, architectures, and standards; design the information infrastructure for utility, resiliency, repairability, and security; develop and implement an IW-D configuration management process; and conduct independent verification of design and procurement specifications to ensure compliance with the design. The SECDEF should:

> **2d(1). Establish a joint security architecture/design office within DISA to shape the design of the DoD information infrastructure.**
>
> **2d(2). Establish a process to verify independently and enforce adherence to these design principles.**

2e. Establish a Red Team for independent assessments. The Red Team would assess the vulnerabilities of new systems and services and would conduct "IW-like" attacks to verify the readiness posture and preparedness of the fighting forces and supporting activities. The SECDEF should:

> **2e(1). Establish a Red Team which is accountable to SECDEF/DEPSECDEF and independent of design, acquisition, and operations activities.**
>
> **2e(2). Develop procedures for employment of the Red Team.**

3. Increase awareness (6.3). The Task Force strongly suggests the need to make senior-level government and industry leaders aware of the vulnerabilities and of the implications. To that end, the SECDEF should:

> **3a. Establish an internal and external IW-D awareness campaign for the public, industry, CINCs, Services, and Agencies.**
>
> **3b. Expand the IW Net Assessment recommended by the 1994 Summer Study to include assessing the vulnerabilities of the DII and NII.**
>
> **3c. Review joint doctrine for needed IW-D emphasis.**
>
> **3d. Explore possibility of large-scale IW-D demonstrations for the purpose of understanding cascading effects and collecting data for simulations.**
>
> **3e. Develop and implement simulations to demonstrate and play IW-D effects (USD(A&T) lead).**

3f. Implement policy to include IW-D realism in exercises.

3g. Conduct IW-D experiments.

4. Assess infrastructure dependencies and vulnerabilities (6.4). Various infrastructures are vitally needed to support mobilization, deployment, and employment of forces and to control and sustain those forces. Some of these interconnected infrastructures are known to have single points of failure. Therefore, the SECDEF should:

4a. Develop a process and metrics for assessing infrastructure dependency.

4b. Assess/document operations plans infrastructure dependencies.

4c. Assess/document functional infrastructure dependencies.

4d. Assess infrastructure vulnerabilities.

4e. Develop a list of essential infrastructure protection needs,

4f. Develop and report to the SECDEF the resource estimates for essential infrastructure protection.

4g. Review vulnerabilities of hardware and software embedded in weapons systems,

5. Define threat conditions and responses (6.5). Conditions analogous to DEFCON should be developed to provide a common understanding of IW threat conditions. Appropriate responses to these conditions should also be developed using the Task Force suggestions outlined in the report as a starting point. The SECDEF should:

5a. Define and promulgate a useful set of IW-D threat conditions which is coordinated with current intelligence community threat condition definitions.

5b. Define and implement responses to IW-D threat conditions.

5c. Explore legislative and regulatory implications.

6. Assess IW-D readiness (6.6). A standardized process is necessary to enable commanders to assess and report their operational readiness status as it relates to their specific dependency on information and information services. Using the standard vocabulary suggested by the Task Force, the SECDEF should:

6a. Establish a standardized IW-D assessment system for use by CINCs, MilDeps, Services, and Combat Support Agencies.

6b. Incorporate IW preparedness assessments in Joint Reporting System and Joint Doctrine, for example.

7."Raise the bar" with high-payoff, low-cost items (6.7). There are a number of low-cost activities the Department can undertake to "raise the bar" significantly for potential systems and network intruders. Three specific Task Force recommendations are that the SECDEF should:

7a. Direct the immediate use of approved products for access control as an interim until a MISSI solution is implemented and for those users not programmed to receive MISSI products.

7b. Examine the feasibility of using approved products for identification and authentication.

7c. Require use of escrowed encryption for critical assets such as databases, program libraries, applications, and transaction logs to preclude rogue employees from locking up systems and networks.

8. Establish and maintain a minimum essential information infrastructure (6.8). A strategy and an overall architecture concept employing existing core capabilities such as Milstar must be developed to serve as a means for restoring services for critical functions and adapting to large- scale outages. The SECDEF should:

8a. Define options with associated costs and schedules.

8b. Identify minimum essential conventional force structure and supporting information infrastructure needs.

8c. Prioritize critical functions and infrastructure dependencies.

8d. Design a Defense MEII and a failsafe restoration capability.

8e. Issue direction to the Defense Components to fence funds for a Defense MEII and failsafe restoration capability.

9. Focus the R&D (6.9). While many commercial and approved security products are available to meet some of the Department's needs, these products generally do not meet the Department's needs in large-scale distributed computing environments and generally do not protect against denial of service attacks. Therefore, the SECDEF should focus the DoD R&D program on the following areas.

9a. Develop robust survivable system architectures.

9b. Develop techniques and tools for modeling, monitoring, and management of large-scale distributed/networked systems.

9c. Develop tools and techniques for automated detection and analysis of localized or coordinated large-scale attacks.

9d. Develop tools for synthesizing and projecting the anticipated performance of survivable distributed systems.

9e. Develop tools and environments for IW-D oriented operational training.

9f. Develop testbeds and simulation-based mechanisms for evaluating emerging IW-D technology and tactics.

In addition, the SECDEF should work with the National Science Foundation to:

9g. Develop research in U.S. computer science and computer engineering programs.

9h. Develop educational programs for curriculum development at the undergraduate and graduate levels in resilient system design practices.

10. Staff for success (6.10). A cadre of high-quality, trained professionals with recognized career paths is an essential ingredient for defending present and future information systems. The Task Force recommends that the SECDEF:

10a. Establish a career path and mandate training and certification of systems and network administrators.

10b. Establish a military skill specialty for IW-D.

10c. Develop specific IW awareness courses with strong focus on operational preparedness in DoD's professional schools.

11. Resolve the legal issues (6.11). The advent of distributed computing has and will continue to further blur the boundaries of the systems and networks that the Department uses. Confusion also stems from uncertainty over when or whether a wiretap approval is needed. Government- wide guidance, and perhaps legislation as well, are needed in the areas of Department assistance to the private sector (e.g., Computer Security Act), tracing attackers of unknown nationality (intelligence versus U.S. persons), tracking attackers through multiple systems, and obtaining/requiring reports of computer-related incidents from the private sector owners and operators of critical infrastructures. The SECDEF should:

11a. Promulgate for Department of Defense systems:

- **Guidance and unequivocal authority for Department users to monitor, record data, and repel intruders in computer systems for self protection,**
- **Direction to use banners that make it clear the Department's presumption that intruders have hostile intent and warn that the Department will take the appropriate response.**
- **IW-D rules of engagement for self-protection (including active response) and civil infrastructure support,**

11b. Provide to the Presidential Commission on Critical Infrastructure Protection proposed legislation, regulation, or executive orders for defending other systems.

12. Participate fully in critical infrastructure protection (6.12). The Task Force makes the following recommendations to the SECDEF regarding the activities of the President's Commission on Critical Infrastructure Protection. Detailed suggestions for each of the below recommendations are outlined in Section 6.12.

12a. Offer specific Department capabilities to the President's Commission.

12b. Advocate the Department's interests to the President's Commission.

12c. Request the Commission provide certain national-level capabilities for the Department,

12d. Suggest IW-D roles for government and the private sector.

13. Provide the resources (6.13). The Task Force reviewed all of the individual recommendations categorized under the key recommendations and estimated to $5 million granularity what the implementation costs might be. The cost estimate is $3.01 billion over fiscal years 1997 through 2001. However, the Department should make a detailed estimate.

[End Executive Summary]

Back to Table of Contents

Credits

Thanks to AR of the Office of Assistant Secretary of Defense (Public Affairs), Department of Defense, for promptly sending this report. For 200-page paper copy telephone: 1-703-697-5737.

Thanks to the IW-D Task Force and contributors.

Published January 8, 1997.

Corrections welcome; send to <jy@jya.com>.